REMARKS

Claims 1, 4, 6-12, 15, 23 and 26 are pending in this application. All of the pending claims are rejected. Claims 1, 6, 12 and 23 are currently amended. Reconsideration is requested.

The presently claimed invention provides scalable security by utilizing group security associations without need for point-to-point tunneling. Group security associations are known for communications common to a group, e.g., multicast. However, point-to-point security associations are used for group security when communications are not common to the group. For example, as explained in the Background at page 2, lines 20-25, VPNs and IPsec tunneling use point-to-point connections between sites. Each secure connection requires storage of association data. Consequently, the amount of data that must be stored to support N point-to-point connections increases at a rate of N^2-1. This presents a scalability problem that is at least mitigated by utilizing a group security association for members of a private network, e.g., store one group security association from the private network rather than individual security associations for each point-to-point or member-to-member connection.

Claims 1, 4, 6-12, 15, 23 and 26 are rejected under 35 U.S.C. 103(a) based on US 2002/0154635 (Liu) in combination with US 6,970,941 (Caronni) and US 6,185,650 (Shimbo). With regard to the limitation of transforming the packet according to a group security association associated with the private network, as recited in the independent claims, the Examiner cites Caronni at column 7, lines 5-33; column 3, lines 17-21; and column 11, lines 37-43. The Examiner explains that "the mappings of the internal/private address, known as node ID, which is considered as a part of the group security association … the security association (SA) is related to Authentication Header (AH) … ." Applicant respectfully traverses. The specification of this application describes a Group Security Association (GSA) at page 11, line 12 through page 12, line 5. In particular, the GSA is a bundling of SAs that together define how a group securely communicates, e.g., selectors, properties, cryptographic policy and keys. Applicant submits that the Examiner's assertion that a mapping between internal and external addresses is analogous to a GSA is fundamentally flawed because such a mapping is neither covered by the description in the specification nor capable of providing any practical measure of security for communications. The cited passage at column 7 describes such an address mapping, and there is no indication in Caronni that the external address is secure or used for a group. Indeed, there is no indication that the mapping is anything more than the result of address resolution for routing purposes. Caronni describes providing security elsewhere, but only point-to-point security techniques which suffer the scalability problem discussed above. For example, the cited passage at column 3 describes "secure communications between nodes," rather than secure communications between all nodes associated with a group using the same GSA. The cited passage at column 11 is unrelated to security. The claims distinguish the cited combination because Caronni fails to describe transforming the packet according to a group security association associated with the private network.[1] As described at page 5, lines 9-10, "with such an arrangement, secure communications can be achieved without the need for point to point tunneling."

The distinguishing feature described above is recited in the independent claims as follows. In claim 1 the feature is recited as "transforming the second portion of the packet according to a group security association associated with the private network to provide a transformed portion which includes a transformed group header." In claim 12 the feature is recited as "applying the group security association to the modified packet to provide a secure

[1] Note that Liu and Shimbo are not cited as showing this novel feature and are therefore not discussed in detail. However, Applicant does not concede the asserted characterizations of those references.

packet including applying the security association to the gateway source address." In claim 23 the feature is recited as "a key table, the key table including a security association for each group for which the node is a member." Claims 4, 6-11, 15, and 26 are dependent claims which further define the invention, and which are allowable for the same reasons as their respective base claims.[2]

Conclusion

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

March 5, 2008
Date

/Holmes W. Anderson/
Holmes W. Anderson, Reg. No. 37272
Attorney/Agent for Applicant(s)
Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-306
Dd: 3/5/2008

[2] This also applies to the additional rejection under 103(a) in which US 2003/0233454 is added to the combination of references.